Appendix A

Summary of Recommendations

We recommend that Corporate Accounting Services:

IT governance

- Regularly review and update policies and procedures in order to provide current and accurate information to users. A history should be maintained to inform users of the changes and the current approved version in use.
- Develop a process to monitor compliance with policies and standards.
- Regularly review job descriptions to make sure that the roles and responsibilities are still current and the skills and experience required are clearly specified.
- Perform a Business Continuation Plan risk analysis and testing annually (or when significant changes occur) and update the plan regularly to ensure its contents are complete and accurate.
- Prepare a quality management plan, defining the quality assurance process and how it will be implemented, for each system project as required by the adopted standards.
- Develop a process to monitor overall information technology performance by comparing actual performance to the capacity and technology plan on a regular basis.

UNIX operating system

- Set the passwords for the production servers to different passwords from those in the test and development environments.

Oracle database

- Identify high-risk information in the Oracle database, implement an audit log—that cannot be altered—that records changes made to this information and assign an individual to review the audit logs regularly and follow up on any unusual activity.

Firewall access

- Restrict access to the test and development servers to only those IP addresses that require access.
- Determine the appropriate IP addresses for access to CAS and restrict the firewall rules accordingly.
- Add a rule to the IP filter that allows only the mainframe IP addresses to use the FTP port on the database server and disables the service on the other servers.
- Add a rule to the IP filter that allows only the TELNET port to be used on the servers that require TELNET.
- Develop a process to notify support staff when the firewall is not running.
- Review, along with Common IT Services, the current firewall single-point of failure configuration to determine if a more secure configuration can be devised.

Appendix B

Office of the Auditor General: 2005/2006 Reports Issued to Date

Report 1 – April 2005

Follow-up of the Recommendations of the Select Standing Committee on Public Accounts contained in its Fourth Report of the 3rd Session of the 36th Parliament: Earthquake; Performance Audit

Report 2 – May 2005

Joint Follow-up of 2001/2002: Report 1 Managing Interface Fire Risks and Firestorm 2003 Provincial Review

Report 3 – June 2005

Audit of the Government's Corporate Accounting System: Part 1

This report and others are available on our website at http://www.bcauditor.com

Compiled and typeset by Graphic Designer, Debbie Lee Sawin, of the Office of the Auditor General of British Columbia
and published by the Queen's Printer for British Columbia©
Victoria 2005